1. Claims 1, 6, 10-11, 14, 16-17, 20 and 22 have been amended. Claims 1-14 and 16-26 have been examined.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 02/04/2010 has been entered.

Response to Arguments

3. Applicant's arguments have been considered but are moot in view of the new ground(s) of rejection.

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

5. Claims 1, 3-4, 10 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Radatti (U.S. Patent 7,389,540; hereafter “Radatti”), and further in view of Szor (U.S. Patent 7,293,290) and further in view of Voelker et al. (U.S. Patent 6,014,513; hereafter "Voelker") and further in view of Schmall (“Classification and identification of malicious code based on heuristic techniques utilizing Meta languages”).

For claims 1 and 20, Radatti teaches a method and apparatus for detecting malicious code in a stream of data traffic input to a gateway of a data network, the method comprising the steps of:

(a) monitoring by the gateway for at least one suspicious portion of data in a portion of the stream of data traffic (note column 5, lines 52-65).

Radatti differs from the claimed invention in that they fail to teach:

Data traffic that is expected to lack executable code.

Szor teaches:

Data traffic that is expected to lack executable code (note column 2, lines 13-21).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the scanner of Radatti with the scanning selected ports for

executable code for further analysis of Szor. One of ordinary skill in the art would have been motivated to combine Radatti and Szor because executable code normally does not appear on certain ports and is therefore suspicious when it is present (note column 2, lines 13-21 of Szor).

The combination of Radatti and Szor differs from the claimed invention in that they fail to teach:

(b) upon detecting said at least one suspicious portion of data, attempting to disassemble said at least one suspicious portion of data thereby attempting to produce disassembled **executable** code; **and**

(c) if said attempting to disassemble said at least one suspicious portion of data succeeds in producing disassembled executable code, then:

Voelker teaches:

(b) upon detecting said at least one suspicious portion of data (note column 2, lines 1-4), attempting to disassemble said at least one suspicious portion of data thereby attempting to produce disassembled **executable** code (note column 7, line 37 through column 8, line 61); **and**

(c) if said attempting to disassemble said at least one suspicious portion of data succeeds in producing disassembled executable code (note column 9, lines 62-67 and column 6, line 28 through column 7, line 28)**, then:**

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of Radatti and Szor and the attempted disassembly of Voelker. One of ordinary skill in the art would have been motivated to combine Radatti, Szor and Voelker because it would provide a method to differentiate between code portions and data portions of a suspicious portion of data (note column 2, lines 16-20 of Voelker).

The combination of Radatti, Szor and Voelker differs from the claimed invention in that they fail to teach:

Wherein for each instruction in said disassembled code,

(**i**) assigning respectively a threat weight for each said instruction; and

(**ii**) accumulating said threat weight to produce an accumulated threat weight.

Schmall teaches:

Wherein for each instruction in said disassembled code,

(**i**) assigning respectively a threat weight for each said instruction (note page 146, "A heuristic engine based on a weight based system…"); and

(**ii**) accumulating said threat weight to produce an accumulated threat weight (note page 146, "A heuristic engine based on a weight based system…").

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of Radatti, Szor and Voelker and the weight

based analyzing system of Schmall. It would have been obvious because a simple substitution of one known element (weight based analyzing of Schmall) for another (pattern matching of Radatti) would yield the predictable results of identifying malicious code.

For claim 3, the combination of Radatti, Szor, Voelker and Schmall teaches claim 1, wherein said monitoring is performed by skipping acceptable data in the stream of data traffic, said acceptable data being consistent with a protocol used by the data stream (note column 5, lines 52-65 of Radatti and column 4, lines 14-19 of Szor).

For claim 4, the combination of Radatti, Szor, Voelker and Schmall teaches claim 3, wherein said acceptable data includes acceptable executable code (note column 5, lines 52-65 of Radatti and column 4, lines 14-19 of Szor).

For claim 10, the combination of Radatti, Szor, Voelker and Schmall teaches claim 1, wherein the stream of data traffic includes an encoded data portion, further comprising the step of, prior to said attempting to disassemble:

(**d**) decoding said encoded data portion (note page 149, "… normalize the given input file..." of Schmall).

6. Claims 8, 11-12, 16-18, 21 and 23-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Radatti, Szor, Voelker and Schmall as applied to claim 1 above, and further in view of Muttik (U.S. Patent 6,775,780).

For claims 11 and 16-17, the combination of Vella and Schmall teaches a method, program storage device and system for detecting malicious code in a stream of data traffic input to a gateway of a data network, the stream of data traffic including data packets, the method comprising the steps of:

(a) monitoring by the gateway for at least one suspicious portion of data in a portion of the stream of data traffic (note column 5, lines 52-65 of Radatti) that is expected to lack executable code (note column 2, lines 13-21 of Szor);

(b) upon detecting said at least one suspicious portion of data (note column 2, lines 1-4 of Voelker), attempting to disassemble said at least one suspicious portion of data thereby attempting to produce disassembled **executable** code (note column 7, line 37 through column 8, line 61 of Voelker); **and**

(c) if said attempting to disassemble said at least one suspicious portion of data succeeds in producing disassembled executable code (note column 9, lines 62-67 and column 6, line 28 through column 7, line 28 of Voelker)**, then:**

for each instruction in said disassembled **executable** code**:**

(**i**) assigning respectively a threat weight for each said instruction (note page 146, "A heuristic engine based on a weight based system…" of Schmall)**,** and

(**ii**) accumulating said threat weight to produce an accumulated threat weight (note page 146, "A heuristic engine based on a weight based system…" of Schmall).

The combination of Radatti, Szor, Voelker and Schmall differs from the claimed invention in that they fail to teach:

wherein said threat weight for each said instruction is selectively either:

(**A**) increased for a legal instruction, and

(**B**) decreased for an illegal instruction.

Muttik teaches:

wherein said threat weight for each said instruction is selectively either:

(**A**) increased for a legal instruction (note column 5, lines 14-21), and

(**B**) decreased for an illegal instruction (note column 5, lines 14-21).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of Radatti, Szor, Voelker and Schmall and the negative and positive weights of Muttik. It would have been obvious because a simple substitution of one known element (negative and positive weights of Muttik) for another (weights only for suspicious activity of Schmall) would yield the predicable results of identifying malicious code (note column 5, lines 20-21 of Muttik).

For claims 8, 12, 18 and 21, the combination of Radatti, Szor, Voelker, Schmall, and Muttik teaches claims 1, 11, 17 and 20, wherein said attempting to disassemble is initiated at a plurality of initial instructions, each of said initial instructions with a different

offset within said at least one suspicious portion of data, and said threat weight is accumulated respectively for each said offset (note column 5, lines 4-20 and column 9, lines 9-17 of Voelker).

For claims 23-26, the combination of Radatti, Szor, Voelker, Schmall, and Muttik teaches claims 8, 12, 18 and 21,

Wherein said attempting to disassemble is initiated at every offset within said at least one suspicious portion of data (note column 5, lines 4-20 and column 9, lines 9-17 of Voelker).

7. Claims 2, 6-7 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Radatti, Szor, Voelker, Schmall and Muttik as applied to claims 1 and 11 above, and further in view of Shipley (U.S. Patent 6,119,236).

For claim 2, the combination of Radatti, Szor, Voelker and Schmall differs from the claimed invention in that they fail to teach:

Wherein said at least one suspicious portion of data contains at least one illegal character in a protocol of the stream of data traffic.

Shipley teaches:

Wherein said at least one suspicious portion of data contains at least one illegal character in a protocol of the stream of data traffic (note column 6, lines 40-46).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of Radatti, Szor, Voelker and Schmall and the protocol monitoring of Shipley. It would have been obvious because combining prior art elements according to known methods would yield the predictable results of identifying an intrusion attempt (note column 6, lines 45-46 of Shipley).

For claim 6, the combination of Radatti, Szor, Voelker, Schmall and Shipley teaches claim 1, further comprising the step of:

(**d**) upon said accumulated threat weight exceeding a previously defined threshold level, performing an action selected from the group of:

(i) generating an alert (note page 146 of Schmall), and

(ii) blocking traffic from the source of the suspicious data (note column 8, lines 5-8 of Shipley).

For claim 7, the combination of Radatti, Szor, Voelker, Schmall and Shipley teaches claim 6, wherein said blocking is solely in the stream of data traffic (note column 8, lines 5-15 of Shipley).

For claim 14, the combination of Radatti, Szor, Voelker, Schmall, Muttik and Shipley teaches claim 11, further comprising the steps of:

(**d**) receiving the data packets input from a wide area network interface of the gateway, thereby building the packets into a virtual stream inside the gateway (note column 5, lines 24-31 of Shipley); and

(**e**) upon said accumulated threat weight exceeding a previously defined threshold level, performing an action selected from the group of:

(i) generating an alert (note page 146 of Schmall), and

(ii) blocking traffic from the source of the suspicious data (note column 8, lines 5-8 of Shipley).

8. Claims 5, 9, 13, 19 and 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Radatti, Szor, Voelker, Schmall and Muttik as applied to claims 1, 11, 17 and 20 above, and further in view of Made (U.S. Patent Application Publication 2002/0056076).

For claim 5, the combination of Radatti, Szor, Voelker and Schmall differs from the claimed invention in that they fail to teach:

wherein upon reaching a branch in said disassembled code, further accumulating said threat weight respectively for each branch option in said disassembled code, thereby producing said accumulated threat weight for each said branch option.

Made teaches:

wherein upon reaching a branch in said disassembled code, further accumulating said threat weight respectively for each branch option in said disassembled code, thereby producing said accumulated threat weight for each said branch option (note paragraph [0042]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of Radatti, Szor, Voelker and Schmall and analyzing both sides of a branch of Made. One of ordinary skill in the art would have been motivated to combine Radatti, Szor, Schmall and Made because analyzing both portions of a branch would provide a more thorough analysis of the executable program.

For claims 9, 13, 19 and 22, the combination of Radatti, Szor, Voelker, Schmall, Muttik and Made teaches claims 1, 11, 17 and 20, wherein said attempting to disassemble is initiated at an initial instruction of an address of previously known offset relative to a vulnerable return address (note paragraph [0042] of Made).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Gil et al. (U.S. Patent 7,702,806) teaches a network gateway monitoring system (note Abstract).

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAVID J. PEARSON whose telephone number is (571)272-0711. The examiner can normally be reached on Monday - Friday, 7:30am - 5:00pm; off every other Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/David J Pearson/
Examiner, Art Unit 2437